

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 19-mj-88


19-131-04

**APPLICATION FOR SEARCH AND  
SEIZURE WARRANT "REDACTED"**

I, Matthew J. Miller, being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation and have reason to believe that within the property fully described in Attachment A, attached hereto and incorporated herein by reference, located in the District of South Dakota, there is now concealed certain property, namely: that fully described in Attachment B, attached hereto and incorporated herein by reference, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of 18 U.S.C. § 1341 (Mail Fraud); 18 U.S.C. §§ 1343 and 1349 (Wire Fraud and Conspiracy to Commit Wire Fraud), and 18 U.S.C. §§ 1956 and 1957 (Money Laundering and Conspiracy to Launder Monetary Instruments).

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.

  
Matthew J. Miller, Special Agent  
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence on the 13<sup>th</sup> day of December, 2019, at Sioux Falls, South Dakota.

  
VERONICA L. DUFFY  
UNITED STATES MAGISTRATE JUDGE

CC Agent  
on L  
AUSA

MJD

**ATTACHMENT A "REDACTED"**

**Property to Be Searched**

The property to be searched is currently in the custody of the Federal Bureau of Investigation in Sioux Falls, South Dakota, and the property is more fully described as:

1. Black Kenneth Cole laptop bag;
2. Samsung Galaxy S9+ Blackphone, IMEI # [REDACTED];
3. Lenovo laptop, serial number [REDACTED];
4. Lenovo laptop, serial number [REDACTED];
5. Toshiba hard drive, serial number [REDACTED];
6. WD Elements hard drive, serial number [REDACTED];
7. "Blackphone" mobile phone, IMEI # [REDACTED];
8. NEXUS LG mobile phone, LG-H791;
9. Sony digital recorder, model ICD-UX560; and
10. Mophie hard drive, serial number [REDACTED].

This warrant authorizes the physical search of Item #1 and authorizes the forensic examination of the listed digital media for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B "REDACTED"**

**Particular Things to be Seized**

All information described below that constitutes fruits, evidence, and instrumentalities of the violations identified in the Affidavit for the time period beginning January 1, 2015, through the present shall be subject to this Search Warrant:

1. Phone call documentation, including incoming, outgoing, missed, or attempted calls along with contact lists and their related identifying information and phone numbers, including deleted contacts along with data access and modification records, which may indicate when or how data is stored or used.

2. Electronic message documentation and content, including sent, unsent, received, or attempted messages whether they are texts, tweets, images, videos, e-mails, or some other form of electronic message, from any proprietary cellular software, or third party application including, but not limited to, applications such as Facebook, Facebook Messenger, Snapchat, and WhatsApp, among others.

3. Subscriber and account information.

4. Digital images, including photographs and/or videos which may tend to show ownership of the electronic devices along with evidence of bank records, wire transfer documents, transaction documents, money order documents, cashier check documents, ledgers, lists of other bank accounts, stolen PII, and other electronic records or media (CD's, DVD's, flash drives, etc.), contact information of others involved in the conspiracy to commit wire fraud and/or conspiracy to launder monetary instruments and the fruits of other crimes, and other evidence relating to a violation of 18 U.S.C. §§ 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy), and 1956 and 1957 (Money Laundering and Conspiracy).

5. Digital documents showing who used or owned the electronic devices at the time the things described in this warrant were created edited, or deleted, including, but not limited to, bills or other business-related documents, correspondence, photographs, phonebooks, documents, and browsing history including saved usernames and passwords.

6. Records that show the use of the internet to communicate with co-conspirators, including, but not limited to, records of Internet Protocol (IP) addresses used, firewall logs, caches, browser history, cookies, "bookmarked" or "favorite" web pages, search terms the user entered into any Internet search engine, and records of user-typed web addresses.

7. Voicemail documentation and content which may tend to show the identity of co-conspirators and/or the objects of the conspiracies to commit wire fraud and/or launder monetary instruments.

8. Global Positioning Satellite (GPS) data which may show travel to or from a location in a particular place and time, which may establish the location of suspect residences and storage facilities, identify co-conspirators, meeting locations, patterns of travel, or associate the user of the device to the offenses listed above in Paragraph 4, or link them to other crimes heretofore unknown.

9. Digital documents or other items tending to identify co-conspirators, clients, investors, customers, and sources, including, but not limited to, contacts, electronic messages, notes, memoranda, photographs, address, and phone books, maps, organizers, or lists of names.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The Government agrees to request another search warrant from the Court before it reviews data from the electronic storage media or electronically stored information seized pursuant to this warrant for purposes unrelated to this investigation or for purposes that may expand the timeframe to dates earlier than January 1, 2015.

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 19-mj-98

19-131-04

**SEARCH AND SEIZURE WARRANT**  
**"REDACTED"**

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement officer or an attorney for the government requests the search of the following property located in the District of South Dakota: that fully described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the property described above, and that such search will reveal property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of 18 U.S.C. § 1341 (Mail Fraud); 18 U.S.C. §§ 1343 and 1349 (Wire Fraud and Conspiracy to Commit Wire Fraud), and 18 U.S.C. §§ 1956 and 1957 (Money Laundering and Conspiracy to Launder Monetary Instruments), as fully described in Attachment B, attached hereto and incorporated herein by reference.

**YOU ARE COMMANDED** to execute this warrant on or before

12-27-19 (not to exceed 14 days)

☒ in the daytime - 6:00 a.m. to 10:00 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the undersigned Judge.

CC ALISA  
Agent

msb



☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized,

☐ for \_\_\_\_\_ days (*not to exceed 30*).

☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

12-13-19 at 1:30pm CST at Sioux Falls, South Dakota  
Date and Time Issued

  
VERONICA L. DUFFY  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A "REDACTED"**

**Property to Be Searched**

The property to be searched is currently in the custody of the Federal Bureau of Investigation in Sioux Falls, South Dakota, and the property is more fully described as:

1. Black Kenneth Cole laptop bag;
2. Samsung Galaxy S9+ Blackphone, IMEI # [REDACTED];
3. Lenovo laptop, serial number [REDACTED];
4. Lenovo laptop, serial number [REDACTED];
5. Toshiba hard drive, serial number [REDACTED];
6. WD Elements hard drive, serial number [REDACTED];
7. "Blackphone" mobile phone, IMEI # [REDACTED];
8. NEXUS LG mobile phone, LG-H791;
9. Sony digital recorder, model ICD-UX560; and
10. Mophie hard drive, serial number [REDACTED].

This warrant authorizes the physical search of Item #1 and authorizes the forensic examination of the listed digital media for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B "REDACTED"**

**Particular Things to be Seized**

All information described below that constitutes fruits, evidence, and instrumentalities of the violations identified in the Affidavit for the time period beginning January 1, 2015, through the present shall be subject to this Search Warrant:

1. Phone call documentation, including incoming, outgoing, missed, or attempted calls along with contact lists and their related identifying information and phone numbers, including deleted contacts along with data access and modification records, which may indicate when or how data is stored or used.

2. Electronic message documentation and content, including sent, unsent, received, or attempted messages whether they are texts, tweets, images, videos, e-mails, or some other form of electronic message, from any proprietary cellular software, or third party application including, but not limited to, applications such as Facebook, Facebook Messenger, Snapchat, and WhatsApp, among others.

3. Subscriber and account information.

4. Digital images, including photographs and/or videos which may tend to show ownership of the electronic devices along with evidence of bank records, wire transfer documents, transaction documents, money order documents, cashier check documents, ledgers, lists of other bank accounts, stolen PII, and other electronic records or media (CD's, DVD's, flash drives, etc.), contact information of others involved in the conspiracy to commit wire fraud and/or conspiracy to launder monetary instruments and the fruits of other crimes, and other evidence relating to a violation of 18 U.S.C. §§ 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy), and 1956 and 1957 (Money Laundering and Conspiracy).

5. Digital documents showing who used or owned the electronic devices at the time the things described in this warrant were created edited, or deleted, including, but not limited to, bills or other business-related documents, correspondence, photographs, phonebooks, documents, and browsing history including saved usernames and passwords.

6. Records that show the use of the internet to communicate with co-conspirators, including, but not limited to, records of Internet Protocol (IP) addresses used, firewall logs, caches, browser history, cookies, "bookmarked" or "favorite" web pages, search terms the user entered into any Internet search engine, and records of user-typed web addresses.



7. Voicemail documentation and content which may tend to show the identity of co-conspirators and/or the objects of the conspiracies to commit wire fraud and/or launder monetary instruments.

8. Global Positioning Satellite (GPS) data which may show travel to or from a location in a particular place and time, which may establish the location of suspect residences and storage facilities, identify co-conspirators, meeting locations, patterns of travel, or associate the user of the device to the offenses listed above in Paragraph 4, or link them to other crimes heretofore unknown.

9. Digital documents or other items tending to identify co-conspirators, clients, investors, customers, and sources, including, but not limited to, contacts, electronic messages, notes, memoranda, photographs, address, and phone books, maps, organizers, or lists of names.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The Government agrees to request another search warrant from the Court before it reviews data from the electronic storage media or electronically stored information seized pursuant to this warrant for purposes unrelated to this investigation or for purposes that may expand the timeframe to dates earlier than January 1, 2015.



believe are necessary to establish probable cause to seize instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), and 1956 and 1957 (Money Laundering and Conspiracy to Launder Monetary Instruments), as detailed in Attachment B, attached hereto and incorporated by reference. The IRS and FBI have been investigating what appears to be a scheme to defraud investors. The investigation, as detailed below, has revealed facts establishing probable cause that evidence, fruits, and instrumentalities of the scheme will be located in the computers, hard drives and phones detailed in Attachment A, attached hereto and incorporated herein by reference.

#### **RELEVANT STATUTES**

4. The application for a Search Warrant, which this Affidavit is offered in support thereof, is being applied to seize instrumentalities, fruits, evidence, more particularly described in Attachment A, for violations of:

- a. 18 U.S.C. § 1343, which makes it a crime to engage in a scheme or artifice to defraud another, and obtain the money and property of another, by false and fraudulent pretenses, that involves a wire transmission and interstate or foreign commerce for the purpose of executing the scheme or artifice.
- b. 18 U.S.C. § 1341, which makes it a crime to engage in a scheme or artifice to defraud another and obtain the money and property of another, by false and fraudulent pretenses, that involves the use of the United States Postal Service.
- c. 18 U.S.C. 1956 which makes it a crime to knowingly conduct or attempt to conduct certain financial transactions to conceal or disguise the nature of, location, source ownership or control of the proceeds of a specified unlawful activity.
- d. 18 U.S.C. 1957 which makes it a crime to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from a specified criminal activity.

#### **OVERVIEW OF INVESTIGATION**

5. A joint FBI/IRS investigation has revealed that, between 2015 and the present, Nathan Peachey and several associates solicited over \$10 million

from victims in multiple states for “humanitarian purposes” promising the investment would be safe and the principal would never be touched. In fact, the money was used to purchase and remodel a luxury home in Norway, to purchase silver coins, to purchase a Mercedes Benz automobile, and to fund various personal purchases. Peachey utilized wire transfers, emails, text messages, and telephonic communications as a part of running and participating in the scheme for which Peachey, along with others, was recently indicted in the District of South Dakota, more fully described in Attachment C, which is attached hereto and incorporated herein by reference. Following the grand jury’s return of the indictment against Peachey, this Court issued an arrest warrant. On December 6, 2019, this Court’s arrest warrant was executed at customs in JFK International Airport in Queens, New York. Peachey was returning from Africa, via Paris, France. Immediately following his arrest, the arresting officers searched Peachey incident to arrest and conducted an international-border search. At the time of his arrest, Peachey possessed the items identified in Attachment A, attached hereto and incorporated by reference. These items were then inventoried and transported to the District of South Dakota. These are the items for which a Search Warrant is being sought.

### **BACKGROUND**

6. The investigation began in October 2016, when the South Dakota Division of Criminal Investigation interviewed Jane and Jim Odle of Lake Norden, South Dakota, who had recently transferred approximately \$700,000 from a bank account in South Dakota to an account controlled by John Rick Winer in New Mexico. The interview revealed the money was an investment in a scheme known as G-47, being run by Winer, who lived in New Mexico, and Nathan Peachey, who lived in Pennsylvania.

7. The IRS and FBI reviewed Bank of America account records showing that, between about 2016 and 2018, WINER received approximately \$2.5 million from the Odle’s and other clients/investors and sent some of this money to Nathan Peachey via an account in the name of Jericho Outreach. Peachey in turn transferred the money to bank accounts in Norway, located at DNB Bank.

8. The FBI and IRS reviewed DNB Bank accounts in Norway to which the money was transferred (account numbers [REDACTED] and [REDACTED] in name of Jericho Outreach) and determined the accounts were controlled by Nathan Peachey and Lubova Burkute. Peachey is listed in these documents as the secretary of Jericho Outreach and Burkute as its treasurer and both were signors on the accounts.

### **INVESTOR INTERVIEWS**

9. The FBI and IRS have interviewed multiple investors in this matter. Examples of three investors who had telephonic and or email communication

with Nathan Peachey are summarized below:

10. The FBI and IRS interviewed Jim and Jane Odle of South Dakota who, in the Spring and early Fall of 2016, invested in G-47, an entity run by Nathan Peachey and John Rick Winer. The Odles invested \$50,000 of their own money and \$562,414.46 of money belonging to Jane's Great Uncle, Marvin Martilla, for whom she served as a power-of-attorney. The Odles spoke with Winer and Peachey by telephone, both of whom assured the Odles that their money was being put in a safe place and would be used in some way to help humanitarian causes, such as providing clean drinking water and helping to reduce poverty. The investment would also return between 10-25 percent the first year and more in following years. Winer and Peachey assured the Odles that their principal investment would never be reduced. The Odles sent their investment to Winer via U.S. Mail. Peachey and Winer told the Odles that they would be able to view statements about their account online but they were never able to do so and no such statements were provided. Winer and Peachey also told the Odles that they could get their money back at any time. In October of 2017, the Odles demanded their money back but have only received \$30,000. The \$30,000 was returned to them from a Jericho Outreach bank account.

11. The FBI and IRS interviewed Robert Moller of Tucson, Arizona. In the Fall of 2016, Moller invested \$784,159.00 into Jericho Outreach, an organization run by Nathan Peachey with the assistance of John Rick Winer. Peachey and Winer told Moller the money would be pooled with other investor money and then leveraged to obtain financing for humanitarian projects. Peachey and Winer further assured Moller that the principal would never be touched and he could get it back at any time. Winer and Peachey also said they would not use his investment money for personal expenses, travel expenses, or administrative expenses related to Jericho Outreach. Moller did not expect his investment money would be used to purchase gold, silver, or foreign currency. Winer and Peachey sometimes gave updates on the projects via phone or email.

12. The FBI and IRS interviewed Mark Jones of Charlotte, North Carolina. In about 2012, Jones invested \$22,000 in a project run by Peachey and Winer, which was known as G-64, an organization dedicated to humanitarian projects. Jones is also aware of approximately 100 other investors. Peachey communicated with Jones and the other investors both by email and by telephone and the group of investors, including Jones, most recently received an email from Nathan Peachey on about November 2, 2019. This email discouraged cooperation with law enforcement. Similarly, about a year ago, a large group of investors received a group text from Nathan Peachey discouraging the investors from working with the FBI.

## **FINANCIAL ANALYSIS**

### **Following the money sent to Winer**

13. The FBI/IRS reviewed domestic bank accounts controlled by John Rick Winer including: Bank of America Acct # ending in 6307, registered to "House of Winer," Bank of America Acct # ending in 0032, registered to "Jacobs Provision Trust," and Wells Fargo Bank Acct # ending in 8887, registered to "AG Enterprises" as well as a bank account controlled by Nathan Peachey, held at Bank of America (Acct # ending in 7170), registered to "Jericho Outreach."

14. This review determined the total amount of money from investors deposited into accounts controlled by Winer was \$2,468,573.46. Of this amount, \$2,056,243.81 was transferred to a Jericho Outreach account at Bank of America controlled by Nathan Peachey; \$283,651.31 appears to have been used personally by Winer, and \$118,000 was returned to investors.

15. Of the \$2,056,243.81 transferred to the Jericho Outreach account at Bank of America controlled by Nathan Peachey, \$1,125,000 was transferred to DNB Bank in Norway (to an account registered to "Jericho Outreach, - Norway"), \$113,166.67 was transferred to DNB Bank in Norway (to an account registered to Lubova Burkute, a Latvian citizen and an associate of Nathan Peachey), \$157,095.50 was wired to JM Bullion to purchase silver coins, \$592,037.84 appears to have been used for personal expenses by Peachey, including equipment for his farm, and \$55,000 appears to have been paid back to investors.

### **Money in the Norway Accounts**

16. The FBI/IRS have reviewed DNB bank records for accounts located in Norway to which investor money was transferred (account numbers [REDACTED] and [REDACTED] in the name Jericho Outreach) and determined the accounts were controlled by Peachey and Burkute. Peachey is listed in these documents as the secretary of Jericho Outreach and Burkute as its treasurer and both were signors on the accounts. The opening application shows Jericho Outreach was a "global distributor of Essential Oils," but it appears the money transferred to the accounts was generated from the investment scheme previously described and not from the sale of Essential Oils.

17. The DNB bank records show that, in addition to the \$1.125 million obtained through Winer (described above in paragraphs 10, 11 and 12), an additional \$5,000,000 was transferred to the Jericho Outreach account at DNB Bank in Norway in June of 2016, from a domestic bank account registered to "The Joseph Project," bringing the total transferred from the US to these accounts to \$6,125,000 between late 2015 and early 2018.



18. The Joseph Project is relevant to a portion of the offense conduct alleged in a currently sealed indictment in the District of South Dakota, charging Peachey and two others with conspiracies to commit wire fraud and launder monetary instruments (CR 19-40097), as more fully set forth in Attachment C, attached hereto and incorporated herein by reference. In addition, The Joseph Project also relates to an active FBI investigation and state prosecution of two other individuals in the State of Arizona. I have reviewed the documents in this FBI file and the investors in that scheme were also told their money would be used to leverage funds for humanitarian causes and their principal was not at risk.

How the money was spent

19. The DNB bank records did not reveal money being spent for humanitarian purposes. Instead, the money appeared to be spent on real and personal property, including silver, a house, and a car as indicated below:

20. Since January of 2018, Peachey purchased approximately \$2,969,150 in *Silver Coins* from the JM Bullion Co. in the United States, using funds from the Jericho Outreach accounts at DNB Bank. The FBI and IRS have examined records concerning the purchase of this silver and determined it was shipped to Oslo, Norway. The Norwegian authorities (acting on a request from the FBI/IRS) have since seized about half of those coins, which were being stored in the house described in paragraph 21 below.

21. In 2017 and 2018, the DNB accounts in the name Jericho Outreach were used to *purchase a house and remodel it*.

- On April 27, 2017, Jericho Outreach purchased a residence at [REDACTED] Sandvika, Norway, in the amount of approximately \$1,330,000. Sales records obtained show Jericho Outreach as the purchaser of the property, and Peachey and Burkute signed the purchase agreement for the residence.
- Between 2017 and 2018, payments in the approximate amount of \$1,163,500 were made to renovate and furnish the residence at [REDACTED] in Sandvika, Norway. The FBI/IRS interviewed the general contractor for the house, Remy Ostuft, who said Lubova Burkute insisted on only the very finest and highest end materials for the remodel.

22. On December 13, 2016, Nathan Peachey purchased, for \$83,000, a *Mercedes Benz GLC250 4M*, using funds from the DNB Jericho Outreach accounts from the Bertel O Steen Mercedes-Benz dealership in Oslo, Norway. In October 2019, Peachey was interviewed by IRS/FBI case agents. Peachey stated

that he used part of the “investment” funds to purchase the vehicle.

23. Peachey stated that The Joseph Project is an “ecclesiastical group” which is “one of the assignments we took on.” Peachey explained, “We took money under an ecclesiastical agreement. There were ecclesiastical terms and conditions. It was an international group and I’m a small part of it.” Peachey stated that money from TJP was deposited into the JERICHO OUTREACH bank account in Norway. Peachey also indicated that the funds were used for “humanitarian purposes;” specifically, he said it had been used first to build a “giant house” which serves as “the international headquarters for the Christian Charity Foundation in Norway” and some of it had been used to purchase silver.

### **ARREST OF NATHAN PEACHEY**

24. I am aware that, on December 6, 2019, Nathan Peachey returned from Guinea to the United States via an aircraft and was taken into custody by the U.S. Customs and Border Patrol Service in John F. Kennedy Airport, located in Queens, New York, based upon a federal arrest warrant issued in this case.

25. I have spoken with Kareem J. McKenzie, the Border Patrol Agent who took Peachey into custody. McKenzie turned Peachey over to the US Marshal’s Service but was left with a laptop bag belonging to Peachey. Peachey’s laptop bag contained several electronic items detailed in Attachment A. Since the Marshal’s do not accept personal property, McKenzie inventoried and turned over the items to the FBI because the warrant came from its investigation.

26. McKenzie informed me that he turned over the following items to the FBI airport office at JFK International:

- Black Kenneth Cole laptop bag;
- Samsung Galaxy S9+ Blackphone, IMEI # [REDACTED];
- Lenovo laptop, serial number [REDACTED];
- Lenovo laptop, serial number [REDACTED];
- Toshiba hard drive, serial number [REDACTED];
- WD Elements hard drive, serial number [REDACTED];
- “Blackphone” mobile phone, IMEI # [REDACTED];
- NEXUS LG mobile phone, LG-H791;
- Sony digital recorder, model ICD-UX560; and
- Mophie hard drive, serial number [REDACTED].

### **USE OF COMPUTERS/PHONES**

27. Based on the foregoing, I believe probable cause exists showing that Nathan Peachey utilized computers and telephones in perpetrating his scheme to defraud based on interviews with Jim and Jane Odle, Jim Moller, and Mark

Hall, each of whom indicated they had telephonic and or email contact with Peachey regarding the scheme (see Paragraphs 10, 11 and 12).

28. Based on the foregoing, I also believe probable cause exists showing that Nathan Peachey utilized computers and telephones in perpetrating his scheme to defraud because I have personally observed emails to and from him concerning the scheme while reviewing materials seized during a search warrant of the house at [REDACTED] Sandvika, Norway.

29. I know that computers, electronic storage devices, and phones may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. In this case, I request permission to search the contents and all electronically stored information within the electronic storage devices described above and in Attachment A, attached hereto and incorporated herein by reference. Based upon the totality of the investigation, I have reason to believe there is probable cause to search above-described electronic storage devices and that the search may recover bank records, wire transfer documents, money order documents, cashier check documents, ledgers, lists of other bank accounts, stolen PII, and other electronic records or media (CD's, DVD's, flash drives, etc.), text messages, electronic-mail messages, and contact information of others involved in the conspiracy to commit wire fraud (18 U.S.C. §§ 1343 and 1349), conspiracy to launder monetary instruments (18 U.S.C. §§ 1956 and 1957), and the fruits of other crimes, including mail fraud, wire fraud, and money laundering, as more fully described in Attachment B, attached hereto and incorporated herein by reference.

30. At the time the aforementioned devices were seized upon Peachey's arrest at JFK, a forensic search of these devices on site was not possible because we did not have the technical equipment required to conduct the search nor a qualified person to do so. It is common practice for these devices to be forensically searched at an offsite location that has the technical personnel and the correct forensic equipment to conduct the search in a controlled setting.

31. Based upon the aforementioned, I am requesting that the court authorize a search of the aforementioned electronic devices at an offsite law enforcement facility that has the technology and capability to conduct the forensic examination. I further request that the examining agency be allowed to examine/search the seized electronic devices at a date and time determined by that agency.

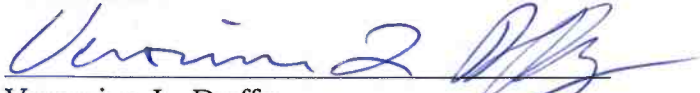
**CONCLUSION**

Based on the information provided, there is probable cause to conclude that evidence, fruits, and instrumentalities of the scheme and criminal offenses, as detailed in Attachment B that is attached hereto and incorporated by reference, that may constitute mail fraud (18 U.S.C. § 1341), wire fraud and conspiracy to commit wire fraud (18 U.S.C. §§ 1343 and 1349), and money laundering and conspiracy to launder monetary instruments (18 U.S.C. §§ 1956 and 1957) will be located in the computers, hard drives, and phones detailed in Attachment A, attached hereto and incorporated herein by reference.



Matthew J. Miller, Special Agent  
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence on the 13<sup>th</sup> day of December, 2019, at Sioux Falls, South Dakota.



Veronica L. Duffy  
United States Magistrate Judge

**ATTACHMENT A "REDACTED"**

**Property to Be Searched**

The property to be searched is currently in the custody of the Federal Bureau of Investigation in Sioux Falls, South Dakota, and the property is more fully described as:

1. Black Kenneth Cole laptop bag;
2. Samsung Galaxy S9+ Blackphone, IMEI # [REDACTED];
3. Lenovo laptop, serial number [REDACTED];
4. Lenovo laptop, serial number [REDACTED];
5. Toshiba hard drive, serial number [REDACTED];
6. WD Elements hard drive, serial number [REDACTED];
7. "Blackphone" mobile phone, IMEI # [REDACTED];
8. NEXUS LG mobile phone, LG-H791;
9. Sony digital recorder, model ICD-UX560; and
10. Mophie hard drive, serial number [REDACTED].

This warrant authorizes the physical search of Item #1 and authorizes the forensic examination of the listed digital media for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B "REDACTED"**

**Particular Things to be Seized**

All information described below that constitutes fruits, evidence, and instrumentalities of the violations identified in the Affidavit for the time period beginning January 1, 2015, through the present shall be subject to this Search Warrant:

1. Phone call documentation, including incoming, outgoing, missed, or attempted calls along with contact lists and their related identifying information and phone numbers, including deleted contacts along with data access and modification records, which may indicate when or how data is stored or used.

2. Electronic message documentation and content, including sent, unsent, received, or attempted messages whether they are texts, tweets, images, videos, e-mails, or some other form of electronic message, from any proprietary cellular software, or third party application including, but not limited to, applications such as Facebook, Facebook Messenger, Snapchat, and WhatsApp, among others.

3. Subscriber and account information.

4. Digital images, including photographs and/or videos which may tend to show ownership of the electronic devices along with evidence of bank records, wire transfer documents, transaction documents, money order documents, cashier check documents, ledgers, lists of other bank accounts, stolen PII, and other electronic records or media (CD's, DVD's, flash drives, etc.), contact information of others involved in the conspiracy to commit wire fraud and/or conspiracy to launder monetary instruments and the fruits of other crimes, and other evidence relating to a violation of 18 U.S.C. §§ 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy), and 1956 and 1957 (Money Laundering and Conspiracy).

5. Digital documents showing who used or owned the electronic devices at the time the things described in this warrant were created edited, or deleted, including, but not limited to, bills or other business-related documents, correspondence, photographs, phonebooks, documents, and browsing history including saved usernames and passwords.

6. Records that show the use of the internet to communicate with co-conspirators, including, but not limited to, records of Internet Protocol (IP) addresses used, firewall logs, caches, browser history, cookies, "bookmarked" or "favorite" web pages, search terms the user entered into any Internet search engine, and records of user-typed web addresses.



7. Voicemail documentation and content which may tend to show the identity of co-conspirators and/or the objects of the conspiracies to commit wire fraud and/or launder monetary instruments.

8. Global Positioning Satellite (GPS) data which may show travel to or from a location in a particular place and time, which may establish the location of suspect residences and storage facilities, identify co-conspirators, meeting locations, patterns of travel, or associate the user of the device to the offenses listed above in Paragraph 4, or link them to other crimes heretofore unknown.

9. Digital documents or other items tending to identify co-conspirators, clients, investors, customers, and sources, including, but not limited to, contacts, electronic messages, notes, memoranda, photographs, address, and phone books, maps, organizers, or lists of names.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The Government agrees to request another search warrant from the Court before it reviews data from the electronic storage media or electronically stored information seized pursuant to this warrant for purposes unrelated to this investigation or for purposes that may expand the timeframe to dates earlier than January 1, 2015.

## ATTACHMENT C "REDACTED"

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

4:19-CR-40097

Plaintiff,

REDACTED INDICTMENT

v.

LOREN WILLIAM ROSIER,  
NATHAN PEACHEY, and  
JOHN RICK WINER,

Conspiracy to Commit Wire Fraud  
18 U.S.C. §§ 1343 and 1349

Conspiracy to Launder Monetary  
Instruments

Defendants.

18 U.S.C. §§ 1956(a)(1)(B)(i) and  
1956(h)

The Grand Jury charges:

COUNT 1

(Conspiracy to Commit Wire Fraud – 18 U.S.C. §§ 1343 and 1349)

Beginning at a time unknown, but no later than on or about 2015, and continuing through the date of this Indictment, in the District of South Dakota and elsewhere, the Defendants, Loren William Rosier, Nathan Peachey, and John Rick Winer, with others known and unknown to the Grand Jury, did conspire to commit the offense of wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349. Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer willfully and unlawfully devised and intended to devise a scheme and artifice to defraud and to obtain money and property from others by means of false and fraudulent pretenses, representations, and promises.

In furtherance of the conspiracy, Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer, and others known and unknown to the Grand

Jury, informed investors that the monies provided to one or more of the co-conspirators would be used for charitable and humanitarian projects and that there would be a return on investments. Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer, and others known and unknown to the Grand Jury, informed investors that the monies provided to one or more of the co-conspirators would not be expended on personal expenses. Investor money was not used for charitable or for humanitarian projects, and investors have not received a return on investments relating to the monies provided to Defendants Loren William Rosier, Nathan Peachey, or John Rick Winer.

As a part of the scheme and artifice to defraud, and in furtherance of the conspiracy, Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer sought and obtained monies, monetary instruments, and money transfers from individuals who were the victims of the scheme. Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer acted willfully, for the purpose of enriching themselves and others, knowing of the unlawful purpose of the scheme, in whole or in part, when they participated in it.

At times relevant to his case, in the District of South Dakota and elsewhere, Defendants William Rosier, Nathan Peachey, and John Rick Winer, and others known and unknown to the Grand Jury, having devised the above-described scheme and artifice to defraud, caused communications to be sent to South Dakota and elsewhere, and did knowingly use and cause communications to be transmitted in interstate or foreign commerce, by means of a wire

communication, writings, signs, signals, and sounds, for the purpose of executing such scheme and artifice.

Defendants' acts and omissions were in violation of 18 U.S.C. §§ 1343 and 1349.

## COUNT 2

(Conspiracy to Launder Monetary Instruments –  
18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h))

Beginning at a time unknown, but no later than on or about 2015, and continuing through the date of this Indictment, in the District of South Dakota and elsewhere, the Defendants, Loren William Rosier, Nathan Peachey, and John Rick Winer, did knowingly and intentionally combine, conspire, confederate, and agree together, with others known and unknown to the Grand Jury, to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, to wit: depositing, transferring, wiring, and withdrawing U.S. Currency at financial institutions, which involved the proceeds of a specified unlawful activity, that is, wire and mail fraud, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, and that while conducting and attempting to conduct such financial transactions Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, all in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h).

FORFEITURE ALLEGATION RELATING TO COUNT 1

The allegations in Count 1 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to 18 U.S.C. § 981(a)(1)(c), and 28 U.S.C. § 2461(c).

Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461, upon conviction of the offense set forth in Count 1 of this Indictment, Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461, any property, real or personal, which constitutes or is derived from proceeds traceable to such violations.

If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

FORFEITURE ALLEGATION RELATING TO COUNT 2

The allegations contained in Count 2 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to 18 U.S.C. § 982(a)(1).

Pursuant to 18 U.S.C. § 982(a)(1), upon conviction of an offense in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(h) as alleged in Count 2 of this Indictment, Defendants Loren William Rosier, Nathan Peachey, and John Rick Winer shall forfeit to the United States of America any property, real or personal, involved in such offense, and any property traceable to such property.

If any of the property described above, as a result of any act or omission of the defendant[s]:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c).



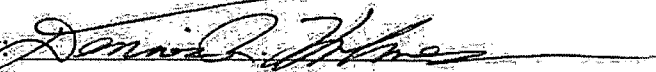
A TRUE BILL:

**Name Redacted**

\_\_\_\_\_  
Foreperson

RONALD A. PARSONS, JR.  
United States Attorney

By

A handwritten signature in dark ink, appearing to read "Dennis R. Holmes", is written over a horizontal line.